Zagadnienia bezpieczeństwa informacyjnego w standardzie TETRA V+D

Rafał Niski

Mirosław Radziwanowski

Omówiono podstawowe zagadnienia dotyczące przeciwdziałania zagrożeniom bezpieczeństwa informacyjnego, uwzględnione w standardzie TETRA V+D, takie jak: procedury uwierzytelniania między infrastrukturą sieciową i stacją ruchomą, kryptograficzne zabezpieczenie informacji przekazywanych przez interfejs radiowy w trybie łączności trankingowej i bezpośredniej, bezpieczne zarządzanie kluczami szyfrującymi, zdalne blokowanie i uaktywnianie terminali oraz mechanizm synchronizacji do szyfrowania informacji w relacji „end-to-end". Ponadto przedstawiono aspekty normalizacji interfejsu LI do legalnego podsłuchu.

TETRA, bezpieczeństwo informacyjne, uwierzytelnianie, szyfrowanie

Wprowadzenie

Podczas opracowywania standardu TETRA duży nacisk położono na zagadnienia związane z bezpieczeństwem informacyjnym, uwzględniając przy tym doświadczenia z eksploatacji wcześniej przygotowanych standardów radiokomunikacji ruchomej GSM i DECT. Wynikało to z potrzeby spełnienia wysokich wymagań różnych użytkowników, a zwłaszcza policji, straży granicznej i innych organizacji bezpieczeństwa publicznego.

Problemy bezpieczeństwa informacyjnego ujęto zarówno w standardzie transmisji głosu i danych (TETRA V+D), jak i w standardzie optymalizowanym pod kątem pakietowej transmisji danych (TETRA PDO). W tym drugim przypadku, z uwagi na specyfikę przekazywanych danych, standaryzacji podlega jedynie mechanizm uwierzytelniania. Z tego względu i z powodu małej popularności standardu TETRA PDO, w artykule omówiono tylko zagadnienia bezpieczeństwa informacyjnego w standardzie TETRA V+D.

Wyszczególnione w tym standardzie zabezpieczenia dotyczą zagrożeń charakterystycznych dla systemów radiokomunikacji ruchomej [1, 6]. Można je podzielić na trzy grupy: zagrożenia dotyczące przekazywanych informacji, zagrożenia dla użytkowników systemu i zagrożenia związane z działaniem samego systemu.

Do zagrożeń, na które są narażone przekazywane informacje można zaliczyć: przechwytywanie informacji, czyli podsłuch (*interception, eavesdropping*), manipulacje informacją (*manipulation*) oraz kwestionowanie odbioru lub autorstwa informacji (*repudiation*). Natomiast zagrożenia dla użytkowników dotyczą głównie nieuprawnionej obserwacji ich zachowań, np. w celu uzyskania informacji o tym, co w danej chwili robią i gdzie się znajdują. Do tej klasy należą takie zagrożenia, jak analiza ruchu (*traffic analysis*) i obserwowalność użytkowników (*observability*). Z kolei systemowi TETRA – jako całości lub jego fragmentom – może zagrażać działanie, polegające na blokowaniu dostępu do usługi (*denial of service*) oraz nieuprawnionym korzystaniu z zasobów (*unauthorized use of resources*).

Zagadnienia bezpieczeństwa łączności w systemie radiokomunikacji ruchomej TETRA były przedmiotem pracy statutowej [7], wykonanej w Samodzielnej Pracowni Radiokomunikacji Morskiej Instytutu Łączności w Gdańsku.

Standardowe funkcje i mechanizmy przeciwdziałania zagrożeniom bezpieczeństwa informacyjnego w systemie TETRA V+D

Uwierzytelnianie stacji ruchomej użytkownika i infrastruktury sieciowej

Przez pojęcie „uwierzytelnianie" rozumie się proces weryfikacji tożsamości i/lub legalności (uprawnień) podmiotu (osoby, obiektu lub systemu). W systemie TETRA realizacja procedur uwierzytelniania ma na celu:

- kontrolę dostępu użytkowników do sieci i przypisanego im zakresu usług;
- zapewnienie prawidłowego rozliczania połączeń (billingu) w sieciach powszechnego użytku;
- wydzielanie unikatowego sesyjnego klucza szyfrującego;
- utworzenie bezpiecznego kanału dystrybucji chronionych informacji, takich jak inne klucze szyfrujące;
- umożliwienie bezpiecznego sterowania zdalnym blokowaniem i uaktywnianiem stacji ruchomych.

W standardzie TETRA przewidziano możliwość uwierzytelniania nie tylko terminalu użytkownika (tak jak w systemie GSM), ale również infrastruktury sieciowej oraz uwierzytelniania wzajemnego obu tych podmiotów.

Procedura uwierzytelniania użytkownika (grupy użytkowników) w stosunku do infrastruktury sieciowej ma zapobiegać nadużyciom, polegającym na podszywaniu się pod innego użytkownika w kanale radiowym („klonowanie stacji ruchomych"), w celu nielegalnego przechwycenia informacji i manipulacji nią lub też nieautoryzowanego wykorzystania zasobów sieci. Pozytywnie zakończona procedura uwierzytelniania powinna poprzedzać świadczenie usług związanych z poufnością, integralnością danych oraz autentycznością pochodzenia danych.

Uwierzytelnianie infrastruktury sieciowej upewni użytkownika o autentyczności infrastruktury sieciowej TETRA. Ma to zapobiegać nadużyciom, polegającym na podszywaniu się pod elementy infrastruktury sieciowej (np. „fałszywa stacja bazowa"), w celu nielegalnego przechwycenia informacji i/lub manipulacji nią. Procedura uwierzytelniania, w zależności od przyjętej polityki bezpieczeństwa, może być wywoływana tylko podczas rejestracji abonenta lub powtarzana wielokrotnie podczas połączenia.

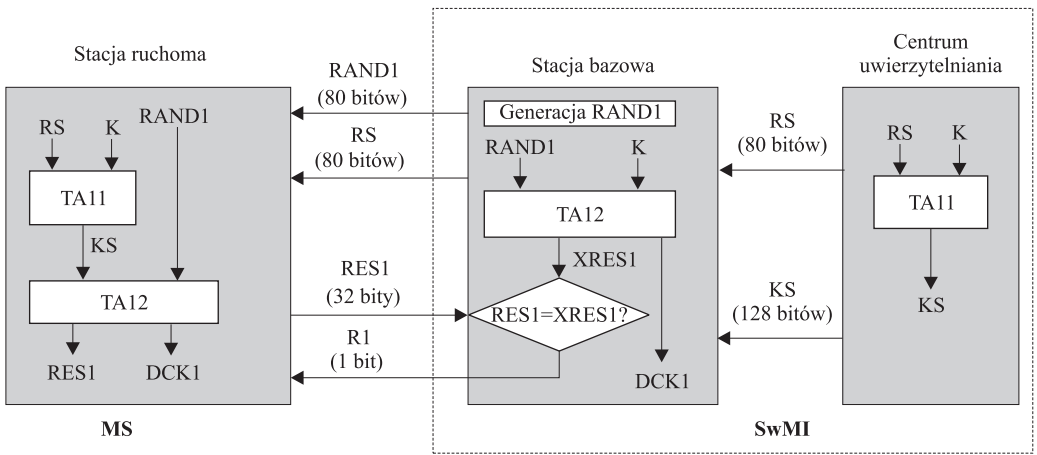
W zastosowaniach wymagających najwyższego poziomu bezpieczeństwa może być uruchamiana procedura uwierzytelniania wzajemnego między użytkownikiem i infrastrukturą.

Uwierzytelnianie stacji ruchomej MS (*Mobile Station*) jest najbardziej powszechną formą uwierzytelniania stosowaną w sieciach TETRA. Procedury uwierzytelniania, w zależności od rodzaju sprzętu, mogą być zaimplementowane albo w terminalu, albo w module TSIM, odpowiedniku karty SIM stosowanej w sieciach GSM.

Przedstawiony na rys. 1 mechanizm uwierzytelniania stacji ruchomej przez infrastrukturę sieciową SwMI (*Switching and Management Infrastructure*) jest oparty na protokole typu „wezwanie-odzew" (*challenge-reaponse*), z wykorzystaniem klucza sesyjnego KS [2].

Klucz KS uzyskuje się z tajnego klucza uwierzytelniania K, który jest współdzielony przez stację ruchomą i infrastrukturę sieciową. Infrastruktura sieciowa SwMI zawiera centrum uwierzytelniania, które przechowuje dane, umożliwiające skojarzenie tajnego klucza K z niepowtarzalnym numerem stacji

ruchomej TEI. Obliczenie wartości klucza KS odbywa się przy użyciu standardowego algorytmu TA11, którego dane wejściowe stanowią tajny klucz K i wartość pseudolosową „zarodka" szyfrowania RS (*Random Seed*).



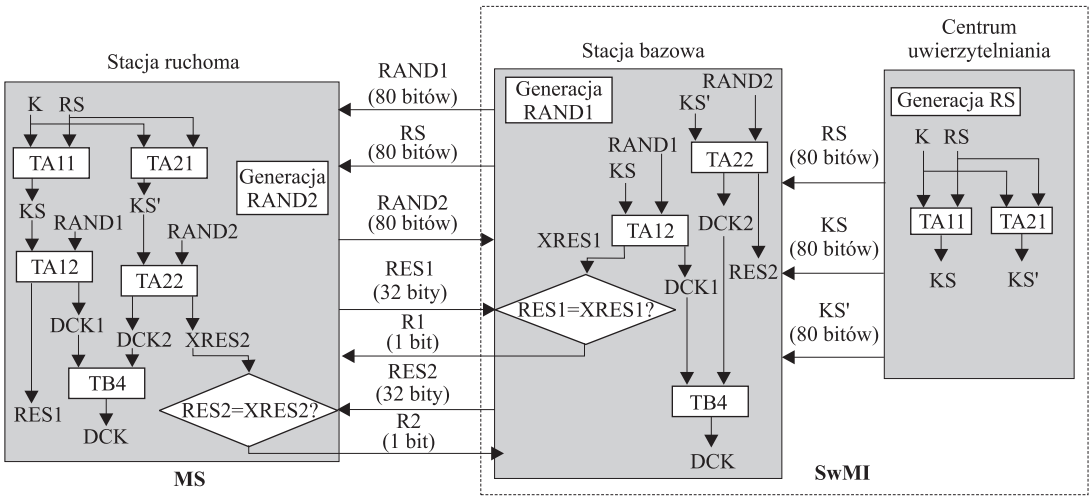
Rys. 1. *Uwierzytelnianie stacji ruchomej przez infrastrukturę sieciową*

W charakterze „wezwania" jest wykorzystywana liczba pseudolosowa RAND1, wygenerowana w SwMI i wysyłana do stacji ruchomej razem z drugą liczbą pseudolosową RS. W stacji ruchomej, na ich podstawie, jest obliczana wartość „odzewu" RES1, natomiast po stronie SwMI – wartość oczekiwana „odzewu" XRES1. Po obu stronach, do wyliczenia „odzewu" jest używany algorytm TA12, za pomocą którego jest generowany również pochodny klucz szyfrujący DCK1. Autentyczność stacji ruchomej zostaje potwierdzona, jeżeli przesłany przez nią „odzew" (RES1) pokrywa się z wartością obliczoną w SwMI (XRES1). Wynik uwierzytelniania R1 jest przesyłany do stacji ruchomej. W podobny sposób, przy odwróceniu kierunków działań („wezwanie" generuje MS), przebiega proces uwierzytelniania infrastruktury, w wyniku którego jest wytwarzany klucz pochodny DCK2.

W procedurze uwierzytelniania wzajemnego stacji ruchomej i infrastruktury wykorzystuje się te same algorytmy i ten sam tajny klucz K, co w przypadku uwierzytelniania jednostronnego. Decyzję o rozpoczęciu uwierzytelniania wzajemnego podejmuje strona „wzywana", a nie „wzywająca". Inaczej mówiąc, uwierzytelnianie takie rozpoczyna się jako jednostronne, inicjowane przez stronę wysyłającą jako pierwsza „wezwanie" i zmienia formę na wzajemne, z inicjatywy strony wysyłającej jako pierwsza „odzew". Jeżeli ta pierwsza procedura uwierzytelniania (jednostronna) zakończy się negatywnie, dalsze działania zostają przerwane.

Na rys. 2 pokazano przykład uwierzytelniania wzajemnego inicjowanego przez SwMI. Tajny klucz uwierzytelniania K oraz wartość RS są wykorzystywane do generacji, przy użyciu algorytmów TA11 i TA21, pary kluczy sesyjnych KS i KS′. Następnie do stacji ruchomej jest wysyłana liczba pseudolosowa RAND1 razem z wartością losową „zarodka" szyfrowania RS. Stacja ruchoma uaktywnia algorytm TA11 w celu wygenerowania klucza sesyjnego KS i – ponieważ uwierzytelnianie ma być wzajemne – algorytm TA21, generujący drugi klucz sesyjny KS′. Stacja ruchoma i SwMI

uruchamiają też algorytm TA12, wytwarzający odpowiednio RES1 i XRES1. Następnie stacja ruchoma wysyła do SwMI „odzew" RES1 i jednocześnie „wezwanie" uwierzytelniania wzajemnego RAND2.



Rys. 2. *Uwierzytelnianie wzajemne inicjowane przez SwMI*

W SwMI następuje porównanie odebranej od MS wartości „odzewu" RES1 z wartością oczekiwaną XRES1 i generacja klucza sesyjnego KS′, przy użyciu algorytmu TA21. W kolejnym kroku SwMI uruchamia algorytm TA22 w celu wytworzenia „odzewu" RES2, będącego reakcją na „wezwanie" stacji ruchomej. „Odzew" RES2 jest wysyłany do MS, gdzie również jest uruchamiany algorytm TA22 do wygenerowania oczekiwanej wartości XRES2. Porównanie wartości XRES2 i RES2 kończy procedurę uwierzytelniania wzajemnego. Pozytywny wynik tego porównania potwierdza autentyczność obu podmiotów uwierzytelniania. Uruchamiane w tej procedurze algorytmy TA12 i TA22 wytwarzają także odpowiednio pochodne klucze szyfrujące DCK1 i DCK2. Proces wzajemnego uwierzytelniania może być również zainicjowany przez MS, wówczas są wykorzystywane te same algorytmy, zmienia się natomiast kolejność działań.

Zarządzanie kluczami kryptograficznymi

Określenie „zarządzanie kluczami" obejmuje generację, dystrybucję, wybór, kasowanie oraz administrowanie kluczami kryptograficznymi, wykorzystywanymi w procesach uwierzytelniania i szyfrowania informacji we wszystkich kanałach telekomunikacyjnych systemu. Do zapewnienia bezpiecznej dystrybucji kluczy jest wymagane przeprowadzenie wcześniej wzajemnego uwierzytelniania podmiotów, które wysyłają i odbierają klucze. Z tego względu procedury zarządzania kluczami i uwierzytelniania muszą być ze sobą ściśle związane.

Tajny klucz uwierzytelniania K jest 128-bitową liczbą pseudolosową jednoznacznie przypisaną do określonego terminalu systemu TETRA lub jego modułu TSIM. Generacja klucza K jest realizowana przez producenta terminalu, dostawcę modułów TSIM lub – w przypadku sieci specjalnego przeznaczenia – przez odpowiednie agencje, zajmujące się bezpieczeństwem. W procesie generacji mogą być wykorzystywane różnego rodzaju generatory liczb losowych. Proces ten powinien odbywać się pod szczególną kontrolą, a uzyskane wyniki muszą być zabezpieczone przed odtajnieniem.

Dystrybucja kluczy uwierzytelniania i powiązanie ich z odpowiednimi adresami sieciowymi są to dwa rozdzielone procesy, realizowane zazwyczaj w różnych momentach czasowych. Dopiero pozytywne zakończenie obu tych procesów umożliwia operacyjne wykorzystywanie kluczy.

Klucze uwierzytelniania są przechowywane po stronie sieciowej w centrum uwierzytelniania, po stronie abonenta zaś w pamięci terminalu lub jego karty TSIM. Powinny one być zabezpieczone przed ujawnieniem lub zniszczeniem. Klucze, które utraciły swoją aktualność, powinny podlegać deaktywacji, co najmniej po stronie sieciowej. W systemach wymagających szczególnie wysokiego poziomu bezpieczeństwa zużyte klucze powinny być niszczone, tzn. fizycznie usuwane z terminalu lub karty TSIM.

Opisane zagadnienia nie są przedmiotem standaryzacji w ETSI. Zajmuje się nimi, działająca w obrębie TETRA MoU, grupa do spraw bezpieczeństwa i zapobiegania nadużyciom SFPG (*Security and Fraud Prevention Group*). Zalecenie TETRA SFPG 01, w którym zaprezentowano wiele mechanizmów bezpiecznej dystrybucji kluczy uwierzytelniania, jest udostępniane członkom TETRA MoU [8, 9].

Bezpieczeństwo informacyjne systemu TETRA opiera się na tajnych kluczach szyfrujących, wykorzystywanych przez odpowiednie algorytmy kryptograficzne. Poważnym problemem jest bezpieczne rozprowadzanie tych kluczy między geograficznie oddalonymi elementami sieci. W tym celu stosuje się wiele mechanizmów zarządzania kluczami oraz sposobów ich generowania. Warto zatem przedstawić podstawowe klucze szyfrujące, zdefiniowane przez standard TETRA V+D, do kryptograficznego zabezpieczania informacji przekazywanych przez interfejs radiowy.

Jak już wspomniano, klucz pochodny DCK (*Derived Cipher Key*) jest wytwarzany podczas realizacji procedury uwierzytelniania i nie jest nigdy przesyłany drogą radiową. Jest to indywidualny, niepowtarzalny klucz szyfrujący, przypisywany dynamicznie do określonego terminalu. Jest on wykorzystywany do szyfrowania transmisji sygnałów głosowych, danych, wiadomości sygnalizacyjnych oraz innych kluczy szyfrujących przesyłanych drogą radiową, tylko w przypadku połączeń indywidualnych.

Klucz wspólny CCK (*Common Cipher Key*) jest generowany przez SwMI i dostarczany do stacji ruchomych w formie zaszyfrowanej przy użyciu indywidualnego klucza DCK. Określenie „wspólny" odnosi się do jednego obszaru ruchowego lub kilku przyległych obszarów. Klucz CCK umożliwia szyfrowanie połączeń grupowych zestawianych ze wszystkimi stacjami ruchomymi, które w danym momencie znajdują się w takim obszarze, niezależnie od tego czy należą one do tej samej zamkniętej grupy użytkowników.

Klucz grupowy GCK (*Group Cipher Key*) jest również generowany przez SwMI i może być dostarczany do stacji ruchomych za pośrednictwem interfejsu radiowego w formie zaszyfrowanej. Klucz taki jest przypisany do jednej zamkniętej grupy użytkowników, co umożliwia kryptograficzne rozdzielenie informacji przekazywanych w różnych grupach. Klucz ten zawsze występuje w formie zabezpieczonej kryptograficznie. W przypadku połączeń grupowych, w danym obszarze ruchowym, zabezpieczenie to polega na szyfrowaniu przy użycia klucza CCK, w celu uzyskania klucza zmodyfikowanego MGCK (*Modified Group Cipher Key*). Natomiast gdy dostarcza się klucz GCK do indywidualnej stacji ruchomej, wówczas zabezpiecza się go sesyjnym kluczem szyfrującym, uzyskiwanym z tajnego klucza uwierzytelniania K.

Klucze statyczne SCK (*Static Cipher Key*) są kluczami generowanymi przez SwMI w zestawach po 32 klucze, a następnie umieszczanymi w bazach danych stacji ruchomych. Określenie „statyczny" oznacza, że wartości tych kluczy nie są zmieniane (np. w procesie uwierzytelniania), aż do momentu ich wymiany przez SwMI na inny zestaw. Klucze SCK mogą być stosowane do zabezpieczania transmisji głosu, danych i informacji sygnalizacyjnych zarówno w połączeniach indywidualnych,

jak i grupowych, w systemach nie stosujących jawnego uwierzytelniania oraz w trybie awaryjnym, jeżeli szyfrowanie kluczami DCK jest niedostępne. Podobnie jak w przypadku kluczy GCK, przesyłanie kluczy SCK do terminalu drogą radiową jest zabezpieczane kryptograficznie przy użyciu sesyjnego klucza szyfrującego.

Standardowy mechanizm wykorzystywany do dystrybucji i uaktualniania drogą radiową kluczy CCK, GCK i SCK, jest określany skrótem OTAR (*Over The Air Re-keying*). Mechanizm ten umożliwia przesyłanie przez interfejs radiowy, w formie zabezpieczonej, kluczy szyfrujących między infrastrukturą SwMI i stacją ruchomą MS. Wiadomości OTAR przesyłane do stacji ruchomej są szyfrowane przy użyciu klucza sesyjnego, który jest uzyskiwany z tajnego klucza uwierzytelniania K danej stacji ruchomej (MS). Szczegółowe diagramy, opisujące protokoły OTAR, realizujące zarządzanie kluczami szyfrującymi przez interfejs radiowy, przedstawiono w [2].

Klasy bezpieczeństwa

Zastosowanie odpowiednich kluczy szyfrujących do szyfrowania informacji przekazywanych przez interfejs radiowy jest ściśle związane z poziomem bezpieczeństwa informacyjnego systemu, definiowanego przez tzw. „klasę bezpieczeństwa". Standard TETRA definiuje, dla trankingowego trybu pracy, trzy klasy bezpieczeństwa.

Najniższy poziom bezpieczeństwa reprezentuje klasa 1, która nie przewiduje szyfrowania informacji w interfejsie radiowym, natomiast zezwala na stosowanie procedury uwierzytelniania.

Dwie pozostałe klasy bezpieczeństwa różnią się rodzajem zastosowanych kluczy szyfrujących. W klasie 2 jest stosowane szyfrowanie przesyłanych informacji oraz skróconych adresów sieciowych przy użyciu klucza statycznego SCK. Procedura uwierzytelniania może być stosowana, ale nie jest to obligatoryjne.

Dla użytkowników najbardziej wymagających została określona klasa 3, zapewniająca najwyższy poziom bezpieczeństwa. W systemie tej klasy mechanizm szyfrowania sygnałów głosowych i danych oraz informacji sygnalizacyjnych wykorzystuje pochodne klucze szyfrujące DCK, z czego wynika obowiązek stosowania procedury uwierzytelniania. W przypadku połączeń grupowych, dla kierunku od SwMI do stacji ruchomej, podstawą szyfrowania jest klucz MGCK w powiązaniu z kluczem wspólnym CCK. Klucz CCK jest używany też do szyfrowania skróconych adresów sieciowych SSI.

Szyfrowanie informacji w interfejsie radiowym

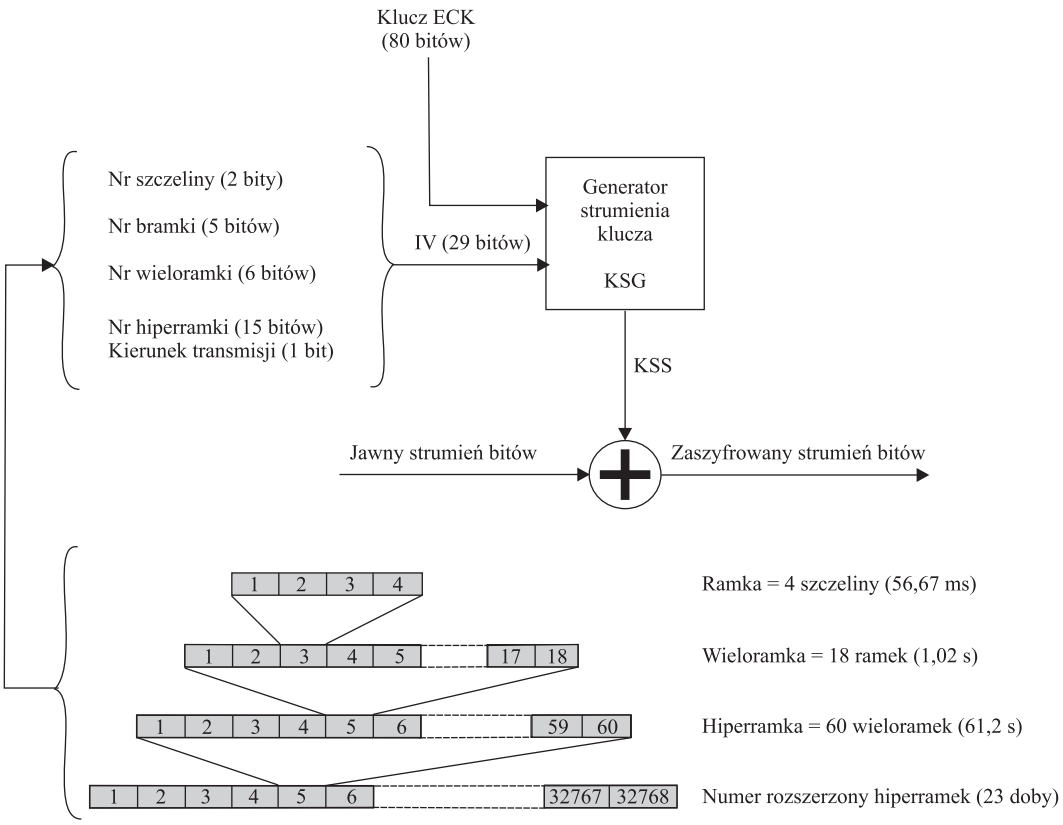
Zaprezentowane różnego rodzaju klucze szyfrujące mogą być wykorzystywane do szyfrowania danych użytkownika i informacji sygnalizacyjnych, transmitowanych w kanale radiowym między stacją ruchomą (MS) i stacją bazową (BS). Szyfrowaniem mogą być objęte zarówno połączenia indywidualne („punkt-punkt"), jak i grupowe („punkt-wiele punktów").

Szyfrowanie informacji w interfejsie radiowym umożliwia dostosowanie bezpieczeństwa informacyjnego w sieciach radiowych do poziomu, jaki zapewniają sieci stacjonarne. Ma ono przeciwdziałać takim zagrożeniom, jak podsłuch oraz analiza ruchu i obserwowalność użytkowników sieci.

Funkcje realizujące szyfrowanie/deszyfrowanie w interfejsie radiowym są ulokowane w górnej części podwarstwy MAC (*Medium Access Control*), wchodzącej w skład warstwy łącza danych (warstwy 2 wg modelu ISO-OSI) stosu protokołów TETRA. Proces szyfrowania po stronie nadawczej poprzedza kodowanie kanałowe, natomiast deszyfrowanie po stronie odbiorczej jest realizowane po dekodowaniu kanałowym.

W procesie szyfrowania/deszyfrowania informacji przekazywanych przez interfejs radiowy są wykorzystywane algorytmy szyfrowania strumieniowego z kluczami symetrycznymi. Szyfrowanie/deszyfrowanie polega na sumowaniu modulo 2 nadawanego/odbieranego ciągu bitów informacyjnych ze strumieniem bitów wygenerowanym z wykorzystaniem specjalnego algorytmu. Taki strumień bitów jest nazywany strumieniem klucza i w standardzie TETRA określa się go skrótem KSS (*Key Stream Segment*). Algorytm generacji klucza KSS jest zaimplementowany w generatorze strumienia klucza KSG (*Key Stream Generator*), który jest integralną częścią zarówno terminali, jak i infrastruktury.

Mechanizm szyfrowania informacji przekazywanych w interfejsie radiowym przedstawiono na rys. 3. Wartości bitów strumienia klucza KSS zależą od klucza utajniania ECK i wektora inicjującego IV (*Initial Value*) generatora KSG. Jak pokazano, 29-bitowy wektor IV jest konstruowany z numerów szczeliny (2 bity), ramki (5 bitów), wieloramki (6 bitów) i hiperramki (15 bitów) struktury czasowej systemu TETRA. Ostatni, 16 bit numeru hiperramek określa kierunek transmisji i jest ustawiany na 0 dla łącza „w dół" i na 1 dla łącza „w górę". Udział 15-bitowego numeru rozszerzającego hiperramek determinuje czas powtarzania strumienia klucza KSS, który wynosi: $2^{15} \cdot 61{,}2$ s $\approx$ 23 doby. Wprowadzenie tak długiego okresu powtarzania KSS powoduje, że analiza zaszyfrowanych danych staje się bardzo trudna, a zatem zapewnia ochronę przed atakami typu *replay*.



Rys. 3. *Mechanizm szyfrowania informacji w interfejsie radiowym*

Klucz utajniania ECK jest wytwarzany na podstawie określonego klucza szyfrującego. W przypadku trzeciej klasy bezpieczeństwa, może to być klucz DCK, CCK lub MGCK, natomiast w drugiej klasie – SCK. W jego generacji biorą udział również dodatkowe parametry, których celem jest randomizacja wartości ECK w obrębie częstotliwości nośnych tej samej komórki i między komórkami w obszarze ruchowym LA.

Standardowe algorytmy kryptograficzne

W systemie TETRA poszczególne grupy użytkowników mogą stosować własne algorytmy szyfrowania, jednak aby zapewnić współpracę systemów opracowanych przez różnych producentów, zdefiniowano kilka algorytmów standardowych o różnym stopniu dostępności. Wyposażenie TETRA, w którym są zaimplementowane algorytmy kryptograficzne podlega restrykcjom eksportowym, zgodnie z zasadami określonymi w porozumieniu o kontroli handlu technologiami o podwójnym zastosowaniu z Wassenaar.

Działający w ETSI eksperci SAGE (*Security Algorithm Group of Experts*) opracowali dwie grupy algorytmów, zaspokajające potrzeby użytkowników o różnym poziomie wymagań odnośnie do bezpieczeństwa informacyjnego:

– algorytmy TEA2 i TEA3, objęte dużymi ograniczeniami eksportowymi;
– algorytmy TEA1 i TEA4, łatwiej dostępne.

Algorytmy z pierwszej grupy są przeznaczone głównie do stosowania przez organizacje bezpieczeństwa publicznego, przy czym TEA2 jest algorytmem wyznaczonym do stosowania przez organizacje krajów, będących sygnatariuszami porozumienia z Schengen, natomiast algorytm TEA3 może być wykorzystywany przez kraje nie objęte tym porozumieniem.

Standardowe algorytmy kryptograficzne TETRA są dostępne dla użytkowników i producentów sprzętu. Udostępnianie algorytmów TEA1, TEA3 i TEA4 odbywa się pod nadzorem ETSI.

Kontrolę nad algorytmem TEA2 sprawuje holenderska policja (*Dutch Police IT organisation*). Licencja na jego stosowanie może być udzielana jedynie instytucjom państwowym do wykorzystania w sieciach związanych z bezpieczeństwem publicznym w takich organizacjach, jak: policja, straż graniczna, straż pożarna, pogotowie medyczne itp.

Ochrona poufności tożsamości użytkowników

System numeracji i adresowania w sieciach TETRA definiuje zastępczy (aliasowy) numer abonenta ATSI (*Alias TETRA Subscriber Identity*), który jest związany z określonym numerem ITSI i może być używany zamiast niego. Możliwość wykorzystywania numeru ATSI do zapewnienia poufności tożsamości abonenta dotyczy również abonentów korzystających z roamingu w sieci wizytowanej, którym jest przydzielany tymczasowy numer ATSI. Informację o powiązaniu pary numerów ITSI – ATSI może mieć jedynie operator sieci. Skrócony numer abonenta SSI może być zastąpiony też numerem zastępczym ASSI (*Alias Short Subscriber Identity*).

Standard TETRA definiuje mechanizm ESI (*Encrypted Short Identity*), który dostarcza środki zabezpieczania informacji identyfikacyjnych transmitowanych w kanale radiowym i może zastępować lub uzupełniać mechanizm ASSI. Nie przewiduje się natomiast stosowania adresów zastępczych (aliasów) w adresach grupowych sieci macierzystej. Mechanizm ESI umożliwia wykorzystywanie aliasów wewnątrz obszaru ruchowego, dla wszystkich typów adresowania. Może on być stosowany tylko

w sieciach, w których informacja przekazywana przez kanał radiowy jest szyfrowana. Mechanizm ESI wykorzystuje klucze CCK, w obszarze ruchowym komórek trzeciej klasy bezpieczeństwa lub klucze SCK komórek drugiej klasy.

Zdalne blokowanie terminali

W standardzie TETRA zostały przewidziane różne rodzaje bezpiecznego zdalnego blokowania i odblokowywania terminali. Możliwe jest zablokowanie wyposażenia terminalu, blokada abonenta w sieci lub użycie obu tych funkcji jednocześnie. Blokowanie wyposażenia opiera się na numerze identyfikacyjnym stacji ruchomej TEI (*TETRA Equipment Identity*), natomiast mechanizm blokowania abonenta wykorzystuje numer identyfikacyjny abonenta w sieci TETRA – ITSI (*Individual TETRA Subscriber Identity*). Zablokowanie wyposażenia (numeru TEI) powoduje, że stacja ruchoma nie może być dłużej używana, nawet jeżeli zostanie wprowadzony inny numer ITSI, który może być zapisany w pamięci wymiennego modułu TSIM. W przypadku zablokowania numeru ITSI stacja ruchoma może być wykorzystywana z innym (aktywnym) numerem ITSI. Wprowadzana blokada może być czasowa z możliwością ponownego uaktywnienia lub trwała, która jest procesem nieodwracalnym.

Bezpieczeństwo informacyjne w trybie łączności bezpośredniej (TETRA DMO)

Stacje ruchome systemu TETRA mogą nawiązywać między sobą łączność bezpośrednią bez udziału infrastruktury sieciowej. Taki rodzaj pracy jest nazywany trybem bezpośrednim i określany skrótem DMO (*Direct Mode Opertion*). W trybie DMO, oprócz prostego połączenia między dwoma terminalami, jest możliwa też łączność ze stacją ruchomą, pracującą w trybie trankingowym z wykorzystaniem techniki podwójnego śledzenia (*dual watch*) lub przez specjalną bramę (*DM-GATE*).

W trybie DMO użytkownik nie może dysponować wszystkimi środkami bezpieczeństwa informacyjnego przewidzianymi dla trybu trankingowego [3]. Nie jest możliwe, np. jawne uwierzytelnianie między terminalami, ponieważ wymagana przez tę procedurę wiedza o tajnym kluczu K jest dostępna tylko w wyposażeniu stacji ruchomej i w infrastrukturze sieciowej. Powoduje to również brak możliwości szyfrowania w interfejsie radiowym z wykorzystaniem kluczy pochodnych DCK. Natomiast jest dostępne szyfrowanie z użyciem kluczy statycznych SCK i uwierzytelnianie domniemane, które polega na tym, że łączność mogą nawiązać między sobą tylko te stacje ruchome, które mają wspólne klucze SCK.

W trybie DMO nie jest stosowana hiperamka, nie występują też pojęcia łącza „w górę” i łącza „w dół”. W związku z tym mechanizm szyfrowania w interfejsie radiowym zamiast wektora inicjującego IV wykorzystuje parametr TVP (*Time Variant Parametr*), który jest transmitowany przez stację ruchomą inicjującą połączenie (stację *master*). Parametr TVP jest liczbą pseudolosową, wybieraną na początku połączenia i następnie inkrementowaną w każdej ramce, z wyjątkiem ramek synchronizacji.

Podobnie jak dla trybu trankingowego, standard TETRA DMO definiuje klasy bezpieczeństwa informacyjnego. W tym przypadku są to cztery klasy: DM-1, DM-2A, DM-2B i DM-2C. Najniższy poziom bezpieczeństwa reprezentuje klasa DM-1, która nie przewiduje szyfrowania informacji i odpowiada klasie 1 w trybie trankingowym. Pozostałe klasy bezpieczeństwa uwzględniają, w różnym stopniu, szyfrowanie danych użytkownika oraz informacji sygnalizacyjnych i adresowych, a także różne konfiguracje połączeń.

Szyfrowanie informacji w relacji *end-to-end*

Wcześniej opisane mechanizmy umożliwiają ochronę danych transmitowanych w interfejsie radiowym oraz uwierzytelnianie użytkownika i/lub infrastruktury sieciowej. Najbardziej narażonym na ataki elementem wszystkich sieci mobilnych jest kanał radiowy, a zatem jego ochrona ma na celu uzyskanie podobnego poziomu bezpieczeństwa informacyjnego jak w sieciach stacjonarnych.

Jeszcze wyższy poziom zabezpieczenia przekazywanych informacji może zapewnić zastosowanie szyfrowania *end-to-end*, obejmującego całe połączenie między terminalami, bez angażowania infrastruktury sieciowej. Wprowadzenie szyfrowania informacji w relacji *end-to-end* nie jest równoznaczne z tym, że stosowanie zabezpieczeń chroniących interfejs radiowy staje się automatycznie niepotrzebne. Korzystanie z pewnych usług, takich jak uwierzytelnianie stacji ruchomej przez infrastrukturę sieciową i odwrotnie lub zdalne blokowanie i odblokowywanie terminali, byłoby niemożliwe bez uaktywniania pewnych zabezpieczeń w interfejsie radiowym. Ograniczenie się wyłącznie do szyfrowania *end-to-end* uniemożliwiłoby ponadto ochronę poufności sekwencji sygnalizacyjnych i w związku z tym również tożsamości użytkownika.

Jednak szyfrowanie informacji w interfejsie radiowym zabezpiecza tylko informacje przekazywane między terminalami i infrastrukturą TETRA. Wewnątrz infrastruktury sieciowej dane są transportowane w formie nie zabezpieczonej. Jest to szczególnie istotne w przypadku, kiedy grupa użytkowników TETRA korzysta z sieci obcego operatora, nie mając pewności, czy ktoś w tej sieci nie podłączył urządzeń podsłuchowych. Dla organizacji szczególnie zainteresowanych zachowaniem poufności przekazywanych informacji, takich jak policja czy inne służby publiczne, taka sytuacja może być nie do zaakceptowania. Tego rodzaju użytkownicy przede wszystkim są zainteresowani szyfrowaniem *end-to-end*.

Standard TETRA nie definiuje ani algorytmów szyfrowania *end-to-end*, ani też metod zarządzania kluczami szyfrującymi. Jest określony jedynie – w ogólnym zarysie – mechanizm szyfrowania, głównie pod kątem metody synchronizacji stosowanych szyfrów strumieniowych, umożliwiając różnym grupom użytkowników implementację własnych rozwiązań dostosowanych do wymaganego poziomu bezpieczeństwa [5]. Mechanizm ten nie ma zastosowania w przypadku szyfrów samosynchronizujących oraz szyfrów blokowych.

Standardowy mechanizm szyfrowania *end-to-end* dotyczy zarówno pracy w trybie trankingowym, jak i DMO. Do synchronizacji transmisji mechanizm ten wykorzystuje kanał STCH (tzw. kanał „kradnący"). Mechanizm szyfrowania *end-to-end* musi spełniać następujące podstawowe wymagania:

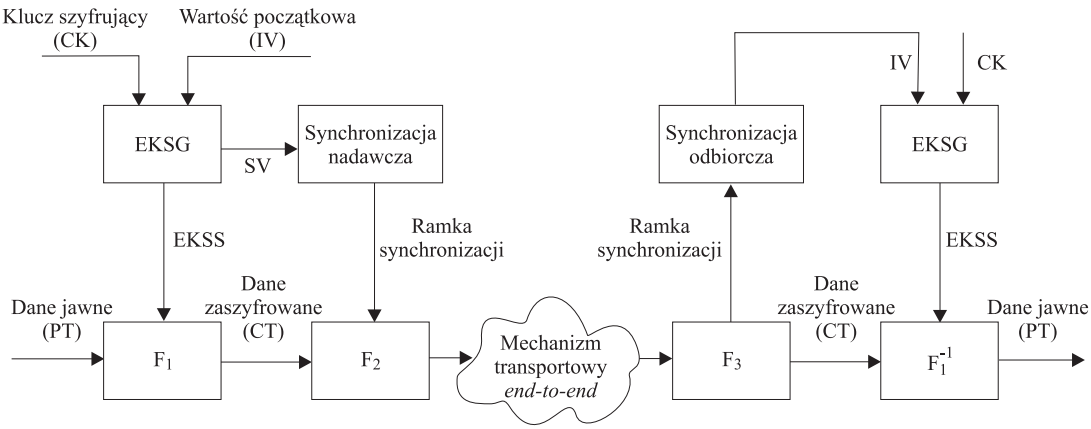
– w obu kierunkach transmisji obowiązuje ten sam mechanizm szyfrowania;
– proces synchronizacji dla każdego kierunku powinien być niezależny;
– procedura szyfrowania *end-to-end* powinna być umieszczona w płaszczyźnie użytkownika (*U-plane*), powyżej procedury szyfrowania w interfejsie radiowym ulokowanej w podwarstwie MAC;
– zależności czasowe i kolejność transmitowanych danych (zarówno w formie jawnej, jak i zaszyfrowanej) powinny być utrzymywane w obrębie par podszczelin (podszczeliny powinny być odtwarzane w tym samym porządku i z tymi samymi warunkami granicznymi na obu końcach łącza).

Warto zaznaczyć, że informacje zaszyfrowane wcześniej w trybie *end-to-end*, mogą zostać ponownie zaszyfrowane za pomocą funkcji obsługujących szyfrowanie w interfejsie radiowym.

Zagadnienia związane z zarządzaniem kluczami szyfrującymi stosowanymi w procesie szyfrowania *end-to-end* nie są przedmiotem standardu TETRA. Zaleca się jednak wykorzystywanie w tym celu usługi transmisji krótkich wiadomości (SDS) z zawartością informacyjną definiowaną przez użytkownika. Wiadomość zarządzania kluczami szyfrującymi powinna zawierać następujące parametry:

– numer klucza szyfrującego;
– tożsamość jednostki szyfrującej;
– klucz kryptograficzny w formie zabezpieczonej.

Mechanizm szyfrowania i deszyfrowania głosu ilustruje schemat funkcjonalny przedstawiony na rys. 4. Jest to mechanizm symetryczny, wykorzystywany zarówno w nadajniku jak i odbiorniku, po obu stronach połączenia.



Rys. 4. *Schemat ogólny mechanizmu szyfrowania i deszyfrowania głosu w relacji „end-to-end”*

Podobnie jak w przypadku szyfrowania w interfejsie radiowym, opisywany mechanizm wykorzystuje generator strumienia klucza EKSG (*End-to-End Key Stream Generator*). Do wejść generatora jest doprowadzany klucz szyfrujący (CK) i wektor wartości początkowej (IV).

Wartość początkowa IV służy do inicjowania działania generatora EKSG. W celu zapobieżenia atakom typu „zarejestruj i powtórz” (*replay*) powinien to być parametr, którego wartość zmienia się w czasie (np. numer kolejny lub znacznik czasu). Z tych samych względów, w charakterze klucza CK może być wykorzystywany klucz szyfrujący pochodny, inny dla każdego połączenia. Na wyjściu generatora EKSG jest wytwarzany segment strumienia klucza EKSS.

Proces szyfrowania jest realizowany przez funkcję F_1, która wykorzystuje strumień klucza EKSS do przetwarzania ciągu bitów reprezentujących dane jawne (PT) na ciąg zaszyfrowany (CT). Funkcja odwrotna F_1^{-1} służy do deszyfrowania, przy użyciu ciągu EKSS, danych zaszyfrowanych (CT) w celu odzyskania danych jawnych (PT). Natomiast zadaniem funkcji F_2 jest podmiana podramki TETRA z danymi CT na ramkę synchronizacji dostarczaną przez moduł funkcjonalny „synchronizacja nadawcza”. Po stronie odbiorczej, funkcja F_3 rozpoznaje ramkę synchronizacji w odbieranym ciągu danych zaszyfrowanych (CT) i dostarcza ją do modułu „synchronizacja odbiorcza”.

Opisywany mechanizm musi być wyposażony w interfejs, który umożliwia sterowanie funkcjami kryptograficznymi i służy do wyboru wartości klucza szyfrującego CK, wyboru numeru wykorzystywanego algorytmu kryptograficznego oraz określenia stanu szyfrowania głosu (włączone/wyłączone).

Jak wspomniano, w standardzie TETRA określono jedynie ogólne ramy bezpieczeństwa *end-to-end*, koncentrując się przede wszystkim na problematyce synchronizacji między modułami szyfrującymi. Dla użytkowników, którzy chcieliby wprowadzić szyfrowanie *end-to-end*, ale nie mają możliwości rozwiązania tego problemu we własnym zakresie, grupa robocza SFPG, utworzona w TETRA MoU, opracowała dwa zalecenia normalizujące szyfrowanie *end-to-end* dla dwóch różnych usług. Zalecenie SFPG 02 dotyczy szyfrowania sygnałów głosowych i zarządzania kluczami, natomiast zalecenie SFPG 07 – szyfrowania krótkich wiadomości tekstowych (usługa SDS). Zalecenia SFPG są udostępniane wyłącznie upoważnionym członkom organizacji TETRA MoU [10].

Interfejs do legalnego podsłuchu LI

Określenie legalny podsłuch (*lawful interception*) oznacza usankcjonowany prawnie dostęp do prywatnej komunikacji, takiej jak połączenia telefoniczne lub poczta elektroniczna. Ogólnie mówiąc, jest to utajniony proces, w którym operator lub dostawca usługi umożliwia uprawnionym podmiotom dostęp do połączeń osób prywatnych lub organizacji. Legalny podsłuch odgrywa ważną rolę jako narzędzie wspomagające instytucje, zajmujące się bezpieczeństwem publicznym i zwalczaniem przestępczości. W większości krajów europejskich na operatorów publicznych sieci telekomunikacyjnych, a nawet niektórych sieci prywatnych, jest nakładany obowiązek umożliwienia legalnego podsłuchu. Prace normalizacyjne prowadzone w ETSI mają ułatwić realizację środków technicznych do legalnego podsłuchu, w sposób uzasadniony ekonomicznie i zgodnie z wymaganiami prawa krajowego oraz ustaleniami międzynarodowymi.

Rys. 5. *Uogólniony model odniesienia organizacji legalnego podsłuchu*

Uogólniony model odniesienia organizacji legalnego podsłuchu zaprezentowano na rys. 5. Struktura legalnego podsłuchu w telekomunikacji jest dwustopniowa i wykorzystuje dwa rodzaje interfejsów:

– interfejs wewnętrzny LI, zrealizowany zgodnie z technologią stosowaną w danej sieci;

– interfejs zewnętrzny, umożliwiający dołączenie środków uprawnionego monitoringu LEMF (*Law Enforcement Monitoring Facility*), należących do organizacji uprawnionej do zarządzania podsłuchu.

Między interfejsami może być wstawiona funkcja pośrednicząca MF (*Mediation Function*), której zadaniem jest dostosowanie formatu dostarczanych wyników podsłuchu do wymagań krajowych.

Przedmiotem normalizacji w ETSI [4] jest jedynie interfejs wewnętrzny LI między infrastrukturą sieci (SwMI) i funkcją pośredniczącą MF.

Dane uzyskane w wyniku legalnego podsłuchu i dostarczane do interfejsu LI powinny obejmować:

– treść wszystkich połączeń inicjowanych przez stację objętą podsłuchem;
– treść wszystkich połączeń adresowanych do stacji objętej podsłuchem;
– treść połączeń grupowych, w których bierze udział stacja objęta podsłuchem;
– treść połączeń w trybie rozgłaszania kierowanych do populacji użytkowników, wśród których znajduje się obiekt podsłuchu.

Oprócz już wymienionych najważniejszych informacji, dane uzyskane w wyniku legalnego podsłuchu powinny też zawierać:

– tożsamość stacji, która próbowała nawiązać połączenie z obiektem podsłuchu, z powodzeniem lub bez;
– tożsamość stacji, z którą próbował nawiązać połączenie obiekt podsłuchu, z powodzeniem lub bez;
– tożsamość wykorzystywaną lub skojarzoną z obiektem podsłuchu;
– wyszczególnienie wykorzystywanych usług i związanych z nimi parametrów;
– sygnały emitowane przez obiekt podsłuchu, które wywołują usługi dodatkowe lub zmodyfikowane;
– znaczniki czasu, umożliwiające określenie początku, końca i czasu trwania połączenia;
– informacje o położeniu stacji podsłuchiwanej.

W celu zapobiegania nadużyciom w wykorzystywaniu środków technicznych, umożliwiających podsłuch, zintegrowanych z systemem TETRA, każdorazowe użycie tych środków powinno być rejestrowane. Operator (dostawca usługi) powinien gwarantować, że zarejestrowane rekordy nie zostały zmodyfikowane i są udostępniane tylko upoważnionym instytucjom, zgodnie z obowiązującym prawem dotyczącym ochrony danych osobowych.

Podsumowanie

Jak wynika z przedstawionego opisu, przy opracowaniu standardu TETRA szczególną uwagę poświęcono zagadnieniom związanym z bezpieczeństwem informacyjnym. Zdefiniowano wiele funkcji i mechanizmów ochronnych, które mogą być wykorzystywane przez poszczególne grupy użytkowników, dostosowując poziom bezpieczeństwa do własnych potrzeb.

Do podstawowych środków bezpieczeństwa informacyjnego zintegrowanych ze standardem TETRA V+D należy zaliczyć:

– uwierzytelnianie użytkownika i infrastruktury sieciowej,
– szyfrowanie informacji przekazywanych przez kanał radiowy,
– szyfrowanie informacji w relacji *end-to-end*,
– utajnianie tożsamości abonentów,
– zdalną blokadę terminali.

Unikatową cechą standardu TETRA jest możliwość kryptograficznego rozdzielenia zamkniętych grup użytkowników dzięki zastosowaniu grupowych kluczy szyfrujących. Uwzględnienie w standardzie wymienionych funkcji i mechanizmów nie gwarantuje jeszcze bezpieczeństwa sieci opartej na systemie TETRA. Bardzo dużo zależy od przyjętej polityki bezpieczeństwa, która powinna być indywidualnie dostosowana do każdej sieci i każdej kategorii użytkowników. Polityka bezpieczeństwa powinna opisywać, jak zdefiniowane w standardzie funkcje bezpieczeństwa mogą być wykorzystywane i jakie dodatkowe elementy bezpieczeństwa powinny zostać wdrożone. Zdefiniowanie odpowiednio wcześnie polityki bezpieczeństwa jest sprawą najważniejszą przy wdrażaniu systemu TETRA.

Istotną częścią polityki bezpieczeństwa jest problematyka zarządzania kluczami kryptograficznymi. Metoda zarządzania kluczami nie jest przedmiotem standaryzacji w obrębie systemu TETRA, ponieważ najlepsze rozwiązania tego problemu zawsze zależą od specyfiki danej sieci. W standardzie TETRA podano jednak wiele funkcji, które wspomagają bezpieczne zarządzanie kluczami.

Warto dodać, że w standardzie TETRA zdefiniowano nie tylko mechanizmy przeciwdziałania podsłuchowi, ale również zajęto się normalizacją wewnętrznego interfejsu LI w celu ułatwienia realizacji środków do legalnego podsłuchu.

Bibliografia

[1] Dunlop J., Grima D., Irvne J.: *Digital Mobile Communications and the TETRA System*. Wiley, 2000
[2] EN 300 392-7 V2.2.1: *Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D)*; Part 7: *Security*. ETSI, 2004
[3] EN 300 396-6 V1.2.1: *Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO)*; Part 6: *Security*. ETSI, 2004
[4] EN 301 040 V2.0.0: *Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface*. ETSI, 1999
[5] EN 302 109 V1.1.1: *Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption*. ETSI, 2003
[6] ETR 086-3 ed. 1: *Trans European Trunked Radio (TETRA) systems; Technical requirements specification*; Part 3: *Security aspects*. ETSI, 1994
[7] Radziwanowski M., Kazenas J., Niski R.: *Bezpieczeństwo łączności w systemie radiokomunikacji ruchomej TETRA*. Gdańsk, Instytut Łączności, 2004
[8] Roelofsen G.: *TETRA security-an overview*, www.tetramou.com
[9] Roelofsen G.: *Practical security in TETRA*, www.tetramou.com
[10] Walther M.: *TETRA end-to-end security*. Technical Report, Ascom, 2001

Rafał Niski

Mgr inż. Rafał Niski (1976) – absolwent Wydziału Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej (2001); pracownik naukowy Instytutu Łączności w Gdańsku (od 2001), kierownik Samodzielnej Pracowni Radiokomunikacji Morskiej w Gdańsku (od 2005); autor kilkunastu publikacji; zainteresowania naukowe: systemy radiokomunikacji ruchomej, radiokomunikacja morska.
e-mail: R.Niski@itl.waw.pl

Mirosław Radziwanowski

Mgr inż. Mirosław Radziwanowski (1941) – absolwent Wydziału Elektroniki Politechniki Gdańskiej (1965); długoletni pracownik naukowy Instytutu Łączności w Gdańsku; autor oraz współautor wielu opracowań konstrukcyjnych, publikacji i projektów wynalazczych; zainteresowania naukowe: cyfrowe systemy telekomunikacyjne, radiokomunikacja morska.
e-mail: M.Radziwanowski@itl.waw.pl